CloudBridge 1.1

2013-06-30 04:31:07 UTC

Contents

CloudBridge 1.1

As a tool for building a cloud-extended data center, the Citrix NetScaler® CloudBridge™ feature is a fundamental part of the Citrix® Cloud framework. This feature can reduce the cost of moving your applications to the cloud, reduce the risk of application failure, and increase network efficiency in your cloud environment.

With the CloudBridge feature, you can create a network bridge (or more than one) connecting one or more cloud computing instances—virtual servers in the cloud—to your network without reconfiguring your network. Cloud-hosted applications appear as though they are running on one contiguous enterprise network.

Setting up a network bridge involves configuring two NetScaler appliances or virtual appliances, one on each side of the bridge. On each appliance, you configure one or more GRE tunnels and configure IPSec on the tunnel or tunnels. You then assign a name to the network bridge and bind the GRE tunnel(s) to it. Optionally, you can bind VLANs and IP addresses to the network bridge.

If you need only one GRE tunnel, you can use an alternative configuration method in which you configure all of the network bridge elements in one dialog box in the configuration utility. You can add more tunnels later.

About the CloudBridge

A network bridge extends layer 2 bridging to connect a NetScaler appliance or virtual appliance residing in a cloud to a NetScaler appliance or virtual appliance on your LAN. The connection is made through an IP tunnel that uses the Generic Routing Encapsulation (GRE) protocol. The GRE protocol provides a mechanism for encapsulating packets, from a wide variety of network protocols, to be forwarded over another protocol. GRE is used to:

- Connect networks running non-IP, nonroutable protocols, such as AppleTalk, Novell IPX, and NetBIOS.
- Bridge across a wide area network (WAN).
- Create a transport tunnel for any type of traffic that needs to be sent unchanged across a different network.

The GRE protocol encapsulates packets by adding a GRE and a GRE IP header to the packets.

CloudBridge supports the use of open-standard Internet Protocol security (IPSec) protocol suite to secure the communication between peers in the CloudBridge.

In a CloudBridge, IPSec ensures:

- Data integrity
- Data origin authentication
- Data confidentiality (encryption)
- Protection against replay attacks

IPSec uses the transport mode in which only the payload of the GRE encapsulates packet is encrypted. The encryption is done by the Encapsulating Security Payload (ESP) protocol. The ESP protocol ensures the integrity of the packet using a HMAC hash function and the confidentiality using a encryption algorithm. After encrypting the payload and calculating the HMAC, an ESP header is generated and is inserted after the GRE IP header and a ESP trailer is inserted at the end of the encrypted payload. An Authentication Header (AH) is also added before the ESP header for data origin authentication of the packet.

CloudBridge also supports the NAT implementation defined in RFC 3947 and 3948 for the CloudBridge peers to communicate with peers behind a NAT device.

To secure their communication, the two peers in the network bridge use the Internet Key Exchange (IKE) protocol in IPSec to:

- Mutually authenticate with each other, using one of the following authentication methods:

- **Pre-shared key authentication**. A text string called a pre-shared key is manually configured on each peer. The pre-shared keys of the peers are matched against each other for authentication. Therefore, for the authentication to be successful, you must configure the same pre-shared key on each of the peers.

- **Digital certificates authentication**. The initiator (sender) peer signs message interchange data by using its private key, and the other receiver peer uses the sender’s public key to verify the signature. Typically, the public key is exchanged in messages containing an X.509v3 certificate. This certificate provides a level of assurance that a peer's identity as represented in the certificate is associated with a particular public key.

- Negotiate to reach agreement on:

  - A security protocol to use, so that each peer sends data in a format that the other recognizes.

  - An encryption algorithm.

  - Cryptographic keys for encrypting data in one peer and decrypting the data in the other.

This agreement upon the security protocol, encryption algorithm and cryptographic keys is called a Security Association (SA). SAs are one way (simplex). For example, when two NetScaler appliances, NS1 and NS2, are communicating by means of IPSec over a CloudBridge, NS1 has two Security Associations. One SA is used for processing out-bound packets, and the other SA is used for processing inbound packets.

SAs expire after a specified length of time, which is called the lifetime. The two peers usie the Internet Key Exchange (IKE) protocol (part of the IPSec protocol suite) to negotiate new cryptographic keys and establish new SAs. The purpose of the limited lifetime is to prevent attackers from cracking a key.

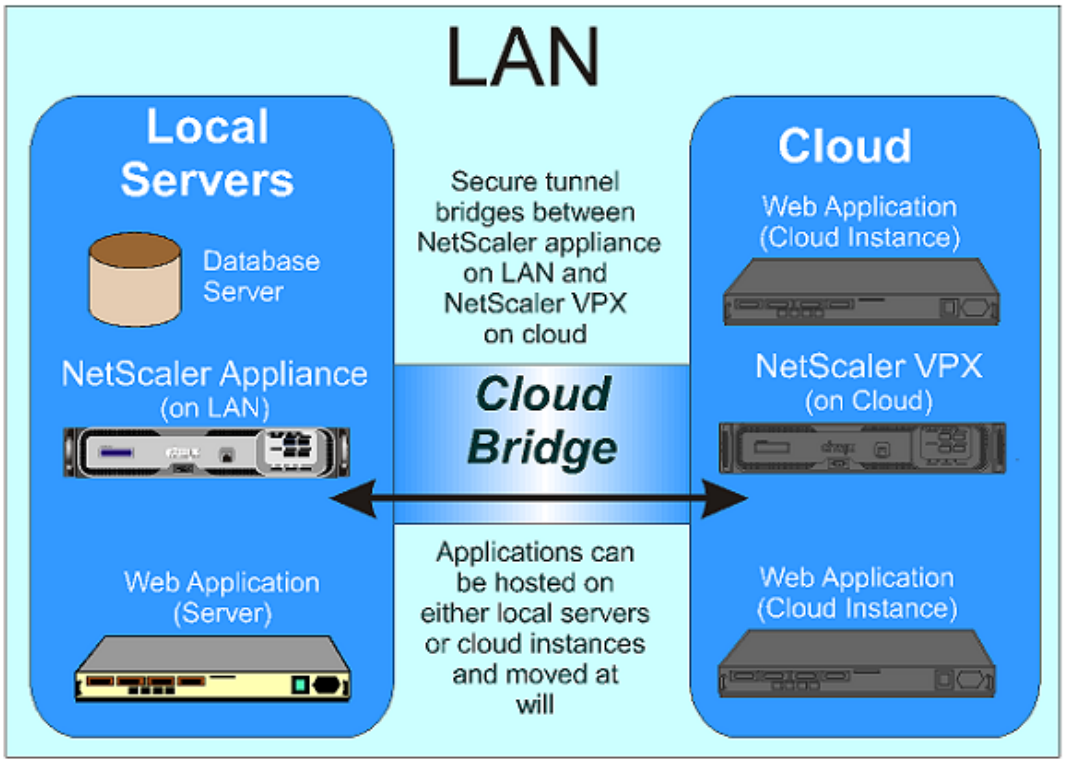

Figure 1. Conceptual Diagram: NetScaler CloudBridge

About the CloudBridge

A network bridge extends layer 2 bridging to connect a NetScaler appliance or virtual appliance residing in a cloud to a NetScaler appliance or virtual appliance on your LAN. The connection is made through an IP tunnel that uses the Generic Routing Encapsulation (GRE) protocol. The GRE protocol provides a mechanism for encapsulating packets, from a wide variety of network protocols, to be forwarded over another protocol. GRE is used to:

- Connect networks running non-IP, nonroutable protocols, such as AppleTalk, Novell IPX, and NetBIOS.
- Bridge across a wide area network (WAN).
- Create a transport tunnel for any type of traffic that needs to be sent unchanged across a different network.

The GRE protocol encapsulates packets by adding a GRE and a GRE IP header to the packets.

CloudBridge supports the use of open-standard Internet Protocol security (IPSec) protocol suite to secure the communication between peers in the CloudBridge.

In a CloudBridge, IPSec ensures:

- Data integrity
- Data origin authentication
- Data confidentiality (encryption)
- Protection against replay attacks

IPSec uses the transport mode in which only the payload of the GRE encapsulates packet is encrypted. The encryption is done by the Encapsulating Security Payload (ESP) protocol. The ESP protocol ensures the integrity of the packet using a HMAC hash function and the confidentiality using a encryption algorithm. After encrypting the payload and calculating the HMAC, an ESP header is generated and is inserted after the GRE IP header and a ESP trailer is inserted at the end of the encrypted payload. An Authentication Header (AH) is also added before the ESP header for data origin authentication of the packet.

CloudBridge also supports the NAT implementation defined in RFC 3947 and 3948 for the CloudBridge peers to communicate with peers behind a NAT device.

To secure their communication, the two peers in the network bridge use the Internet Key Exchange (IKE) protocol in IPSec to:

- Mutually authenticate with each other, using one of the following authentication methods:

- **Pre-shared key authentication**. A text string called a pre-shared key is manually configured on each peer. The pre-shared keys of the peers are matched against each other for authentication. Therefore, for the authentication to be successful, you must configure the same pre-shared key on each of the peers.

- **Digital certificates authentication**. The initiator (sender) peer signs message interchange data by using its private key, and the other receiver peer uses the sender’s public key to verify the signature. Typically, the public key is exchanged in messages containing an X.509v3 certificate. This certificate provides a level of assurance that a peer's identity as represented in the certificate is associated with a particular public key.

- Negotiate to reach agreement on:

  - A security protocol to use, so that each peer sends data in a format that the other recognizes.

  - An encryption algorithm.

  - Cryptographic keys for encrypting data in one peer and decrypting the data in the other.

This agreement upon the security protocol, encryption algorithm and cryptographic keys is called a Security Association (SA). SAs are one way (simplex). For example, when two NetScaler appliances, NS1 and NS2, are communicating by means of IPSec over a CloudBridge, NS1 has two Security Associations. One SA is used for processing out-bound packets, and the other SA is used for processing inbound packets.

SAs expire after a specified length of time, which is called the lifetime. The two peers usie the Internet Key Exchange (IKE) protocol (part of the IPSec protocol suite) to negotiate new cryptographic keys and establish new SAs. The purpose of the limited lifetime is to prevent attackers from cracking a key.

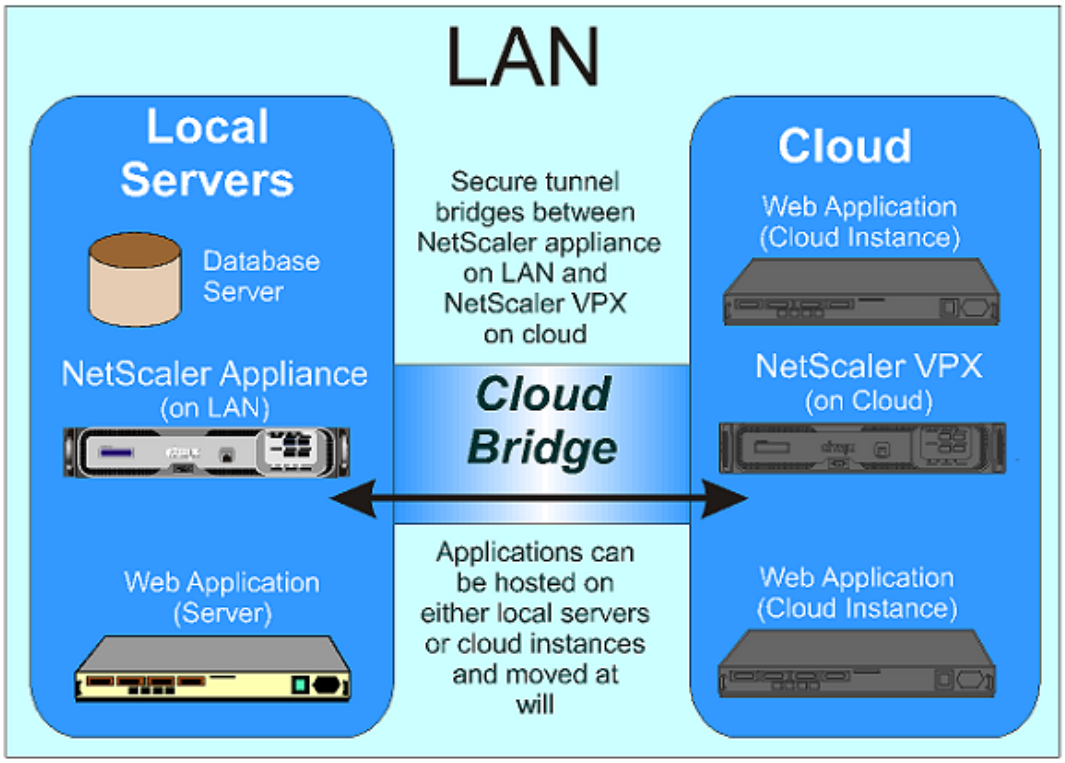

Figure 1. Conceptual Diagram: NetScaler CloudBridge

Setting Up a CloudBridge - Method 1

Before setting up a CloudBridge, you must configure the NetScaler appliance or VPX virtual appliance on the LAN and the appliance or virtual appliance on the Cloud.

To configure a new NetScaler appliance, see Getting Started with Citrix NetScaler. To configure a new virtual appliance, see Getting Started with Citrix NetScaler VPX.

You must then configure networking on both appliances. Each of the two configurations may include a VLAN that contains the servers or the cloud instances that will use the CloudBridge. To configure VLANs, see Configure a VLAN.

To set up a CloudBridge, on the NetScaler appliance or virtual appliance that anchors the LAN side of the CloudBridge:

1. Configure IPSec on the GRE tunnel.
2. Configure a GRE tunnel.
3. Configure a CloudBridge:
    - Create a logical representation of the CloudBridge by specifying a name.
    - Bind one or more GRE tunnels to the CloudBridge.
    - Bind VLANs and IP addresses to the CloudBridge (Optional.)

You then repeat these steps on the NetScaler appliance or virtual appliance that anchors the cloud side of the CloudBridge.

You can perform these tasks individually (Method 1), or you can configure everything in one dialog box in dialog box in the configuration utility (Method 2). For more information, see Setting Up a CloudBridge – Method 2.

Configuring IPSec on a GRE tunnel

For configuring IPSec on a GRE tunnel:

- The **IPSecprofile** parameter should be enabled on the GRE tunnel.
- You need to specify the same local IP address and the remote IP address that you specified for the GRE tunnel.

To configure IPSec on a GRE tunnel by using the NetScaler command line

At the NetScaler command prompt, type:

add ipsec profile <name> [**-encAlgo** (AES | 3DES) ...] [**-hashAlgo** <hashAlgo> ...] [**-lifetime** <positive_integer>] (**-psk** |(**-publickey** <string> **-privatekey** <string> **-peerPublicKey** <string>))

To remove an IPSec config by using the NetScaler command line

To remove an IPSec config, type the rm ipsec profile command and the name of the IPSec config.

Parameters for configuring IPSec on a GRE tunnel

name

Name for an IPSec configuration. The name can begin with a letter, number, or the underscore symbol, and can consist of from one to 127 letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore (_) symbols.

encAlgo

The encryption algorithm to be used in IPSec configuration for a CloudBridge. Possible values: AES, 3DES.

hashAlgo

The encryption algorithm to be used in IPSec configuration for a CloudBridge. Possible values: HMAC_SHA1, HMAC_SHA256, HMAC_MD5. Default: HMAC_SHA1.

lifetime

Time, in seconds, after which the security association expires. After expiration, new SAs are established, and new cryptographic keys are negotiated between the peers connected by the CloudBridge. Maximum value: 31536000. Default: 28800.

psk

A text string, called the pre-shared key, to be manually configured on each peer. The pre-shared keys of the peers are matched against each other for authentication before security associations are established. Therefore, for the authentication to be successful, you must configure the same pre-shared key on both of the peers of the CloudBridge. Maximum Length: 63 characters.

livenessCheckInterval

Time, in seconds, after which a notify payload is sent to check the status of the peer (UP or DOWN). Additional payloads are sent as per the retransmit interval setting. Zero value disables liveliness checks.

retransmissiontime

Time, in seconds, after which IKE retry message is sent to a peer. The retry message is sent three times, each time doubling the time interval for every failure.

publickey

A local digital certificate to be used to authenticate the local NetScaler appliance to the remote peer before establishing IPSec security associations. The same certificate should be present and set for the Peer Public Key parameter in the remote peer.

privatekey

The private key of the local digital certificate.

peerPublicKey

A digital certificate of the remote peer. This certificate is used to authenticate the remote peer to the local peer before establishing IPSec security associations. The same certificate should be present and set for the Public key parameter in the remote peer.

To configure IPSec on a GRE tunnel by using the configuration utility

1. In the navigation pane, expand **CloudBridge**, expand **Advanced**, and then click **IPSec Profile**.
2. In the details pane, click **Add**.
3. In the **Create IPSec Profile** dialog box, type or select values for the following parameters, which correspond to parameters described in "Parameters for configuring IPSec" as shown:
   - **Name*** —name
   - **Encryption Algorithm**—encAlgo
   - **Hash Algorithm**—hashAlgo
   - **Lifetime**—lifetime
   - **Liveness Check Interval**—livenessCheckInterval
   - **Retransmit Interval**—retransmissiontime
   - **Pre-Shared key Exists**—psk
   - **Public Key**—publickey
   - **Private Key**—privatekey
   - **Peer Public Key**—peerPublicKey

   * A required parameter.
4. Click **Create**, and then click **Close**.

Creating IP Tunnels

To create an IP tunnel by using the NetScaler command line

At the NetScaler command prompt type:

- add iptunnel <name> <remoteIp> <remoteSubnetMask> <localIp> **-type** -**protocol** (ipoverip | GRE) -**ipsecprofile** <name>
- show iptunnel

To remove an IP tunnel by using the NetScaler command line

To remove an IP tunnel, type the rm iptunnel command and the name of the tunnel.

Parameters for creating an IP tunnel

name

Name of the IP Tunnel. This alphanumeric string is required and cannot be changed after the service group is created. The name must not exceed 127 characters, and the leading character must be a number or letter. The following characters are also allowed: @ _ - . (period) : (colon) # and space ( ).

remoteIp

A public IPv4 address of the remote NetScaler appliance used to set up the tunnel.

remoteSubnetMask

Subnet mask of the remote IP address of the tunnel.

localIp

A public IPv4 address of the local NetScaler appliance used to set up the tunnel. Possible values: Auto, MIP, SNIP, and VIP. Default: Auto.

protocol

The protocol to be used in setting up the IP tunnel. Select GRE for using the Generic Routing Encapsulation (GRE) protocol to set up a GRE tunnel.

ipsecProfileName

Name of the IPSec profile that is used for securing communication in the GRE tunnel.

To create an IP Tunnel by using the configuration utility

1. In the navigation pane, expand **Network**, and click **IP Tunnels**.
2. In the details pane, click **Add**.
3. In the **Add IP Tunnel** dialog box, specify values for the following parameters:
   - **Name*—**name
   - **Remote IP*—**remoteIp
   - **Remote Mask*—**remoteSubnetMask
   - **Local IP Type***—localIp (in the **local IP Type** drop down list, select one of the IP type (Mapped IP, Subnet IP, and Virtual). All the configured IPs of the selected IP type will be populated in the **Local IP** drop down list. Select the desired IP from the list.)
   - **Protocol—**protocol and ipsecProfileName from the corresponding field when you select protocol as GRE.

   *A required parameter.
4. Click **Create**, and then click **Close.**

To create an IPv6 tunnel by using the NetScaler command line

At the NetScaler command prompt type:

- add ip6tunnel <name> <remoteIp> <local>
- show ip6tunnel

To remove an IPv6 tunnel by using the NetScaler command line

To remove an IPv6 tunnel, type the rm ip6tunnel command and the name of the tunnel.

Parameters for creating an IPv6 tunnel

name (Name)

A name for the IPv6 Tunnel. This alphanumeric string is required and cannot be changed after the service group is created. The name must not exceed 127 characters, and the leading character must be a number or letter. The following characters are also allowed: @ _ - . (period) : (colon) # and space ( ).

remoteIp (Remote IP)

An IPv6 address of the remote NetScaler appliance used to set up the tunnel.

localIp (Local IP Type)

An IPv6 address of the local NetScaler appliance used to set up the tunnel. Possible values: SNIP6 and VIP6. Default: Auto.

To create an IPv6 Tunnel by using the configuration utility

1. In the navigation pane, expand **Network**, and click **IP Tunnels**.
2. On the **IPv6 Tunnels** tab, click **Add**.
3. In the **Create IPv6 Tunnel** dialog box, set the following parameters:
   - **Name***
   - **Remote IP***
   - **Local IP Type*** (In the **local IP Type** drop down list, select one of the IP type (SNIP6 or VIP6). All the configured IPv6 addresses of the selected IPv6 type are be populated in the **Local IP** drop down list. Select the desired IP from the list.)

   *A required parameter.
4. Click **Create**, and then click **Close.**

Configuring a CloudBridge

You can think of the CloudBridge as a group that holds a set of secure GRE tunnels. After configuring GRE tunnels secured with IPSec, you need to create a logical representation of the CloudBridge by assigning a name to a CloudBridge and binding one or more configured GRE tunnels to the CloudBridge. You can then bind VLANs and IP subnets to the new CloudBridge. The VLAN and IP subnet settings are common to all the GRE tunnels bound to the CloudBridge.

To create a CloudBridge by using the NetScaler command line

At the NetScaler command prompt, type:

add netbridge <name>

To bind GRE tunnels, VLANs, and IP Subnets to a CloudBridge by using the NetScaler command line

At the NetScaler command prompt, type:

bind netbridge <name> [**-tunnel** <name>] [**-vlan** <id>] [**-IPAddress** <ip_addr|ipv6_addr>]

To modify or remove an CloudBridge by using the NetScaler command line

- To modify a CloudBridge, type the set netbridge command, the name of the CloudBridge, and the parameters to be changed, with their new values.
- To remove a CloudBridge, type the rm netbridge command and the name of the CloudBridge.

Parameters for configuring a CloudBridge

name

The name of the CloudBridge that you are configuring. The name can begin with a letter, number, or the underscore symbol, and can consist of from one to 127 letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore (_) symbols. You should choose a name that will make it easy for others to tell which NetScaler appliances the CloudBridge connects.

tunnel

The name of the GRE tunnel to be associated with the CloudBridge.

VLAN

The ID of the local VLAN that needs to be extended to the cloud.

IPAddress

The IPV4 subnet that needs to be extended to the cloud.

To configure a CloudBridge by using the configuration utility

1. In the navigation pane, expand **CloudBridge**, and then click **Network Bridge**.
2. In the details pane, do one of the following:
   - To create a new CloudBridge, click **Add**.
   - To modify an existing CloudBridge, select the CloudBridge, and then click **Open**.
3. In the **Create Network Bridge** dialog box, type a name for your new CloudBridge.
4. In the **Create Network Bridge** or **Configure Network Bridge** dialog box, on the **Tunnels** tab (selected by default), do one of the following to bind GRE tunnels to the CloudBridge:
   - If the GRE tunnels that you want are listed, select the corresponding check boxes.
   - If you want bind all the GRE tunnels listed, click **Activate All**.
   - If you want to create a new GRE tunnel, click **Add**.
5. In the **Create Network Bridge** or **Configure Network Bridge** dialog box, on the **VLANs** tab (selected by default), do one of the following to bind GRE tunnels to the CloudBridge:
   - If the VLANS that you want are listed, select the corresponding check boxes.
   - If you want bind all the VLANs listed, click **Activate All**.
   - If you want to create a new VLAN, click **Add**.
6. On the **IP Subnets** tab, do the following to bind IP subnets to the CloudBridge:
   - If you want to bind a new IP subnet, click **Add**.
   - If you want to modify an existing IP subnet, click **Open**.
7. Click **Create**, and then click **Close**.

Configuring the CloudBridge—Method 2

For configuring a network bridge, you need to perform the following steps on each of the appliances that is to a be peer on the network bridge.

1. Configure a GRE tunnel.
2. Configure IPSec on the GRE tunnel.
3. Create a logical representation of the network bridge by specifying a name.
4. Bind one or more GRE Tunnels to the network bridge.
5. Bind VLANs and IP addresses to the network bridge (Optional.)

The configuration utility provides a single dialog box in which you can perform all of these tasks to configure a CloudBridge.

When you use this dialog box:

- A GRE tunnel, IPSec, and network bridge entities are created, all with the same name.
- The GRE tunnel created is configured with IPSec.

By using this method, you can configure a network bridge with only one GRE tunnel. You can later modify the network bridge to bind more GRE tunnels to it.

Parameters for configuring a network bridge

name

The name of the CloudBridge that you are configuring. The name can begin with a letter, number, or the underscore symbol, and can consist of from one to 127 letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore (_) symbols. You should choose a name that will make it easy for others to know which NetScaler appliances the CloudBridge connects.

Local IP

A public IPv4 address of the local NetScaler appliance or VPX virtual appliance. This address is used to set up a GRE tunnel, with IPSec configuration, to a public IP IPv4 address of the remote peer NetScaler appliance or virtual appliance.

Remote IP

A public IPv4 address of the remote peer NetScaler appliance or virtual appliance. This is the address that is used to at the remote peer to set up the GRE tunnel, with IPSec configuration, with the local peer.

Pre-Shared key

A text string, called the pre-shared key, to be manually configured on each peer. The pre-shared keys of the peers are matched against each other for authentication before security associations are established. Therefore, for the authentication to be successful, you must configure the same pre-shared key on both of the peers of the CloudBridge. Maximum Length: 63 characters.

Public key

A local digital certificate to be used to authenticate the local NetScaler appliance to the remote peer before establishing IPSec security associations. The same certificate should be present and set for the Peer Public Key parameter in the remote peer.

Private Key

The private key of the local digital certificate.

Peer Public Key

A digital certificate of the remote peer. This certificate is used to authenticate the remote peer to the local peer before establishing IPSec security associations. The same certificate should be present and set for the Public key parameter in the remote peer.

To configure a CloudBridge by using the configuration utility

1. In the navigation pane, click **CloudBridge**.
2. In the details pane, under Getting Started, click **Configure CloudBridge**.
3. In the **Configure CloudBridge** dialog box, specify values for the following parameters, which are described in "Parameters for configuring a CloudBridge":
   - **Name***
   - **Local IP***
   - **Remote IP***

   * A required parameter.
4. Do one of the following to select an IPSec authentication method between the peers for establishing IPSec security associations:
   - For pre-shared key authentication method, select **Pre-shared Key** and specify values for the following parameters, which are described in "Parameters for configuring a CloudBridge":
     - **Pre-Shared key**
     - **Confirm Key**

     * A required parameter.
   - For digital certificates authentication method, select **Certificate** and specify values for the following parameters, which are described in "Parameters for configuring a CloudBridge":
     - **Public Key**
     - **Private Key**
     - **Peer Public Key**

     * A required parameter.
5. Click **Create**, and then click **Close**.

Setting Up CloudBridge to SoftLayer Enterprise Cloud

The configuration utility includes a wizard that helps you to easily configure a CloudBridge between a NetScaler appliance on any network and NetScaler VPX instances on the SoftLayer enterprise cloud.

Using the wizard, you can perform the following steps to configure a CloudBridge to a NetScaler VPX instance on the SoftLayer enterprise cloud.

1. Connect to the SoftLayer enterprise cloud by providing the user log on credentials.
2. Select the Citrix XenServer that is running the NetScaler VPX appliance.
3. Select the NetScaler VPX appliance.
4. Provide CloudBridge parameters to:
    - Configure a GRE Tunnel.
    - Configure IPSec on the GRE tunnel.
    - Create a logical representation of the CloudBridge by specifying a name.
    - Bind the GRE Tunnel to the CloudBridge.

When you use this wizard, a GRE tunnel, IPSec, and CloudBridge entities are created on both of the peers.

To configure a CloudBridge by using the configuration utility

1. In the navigation pane, click **CloudBridge**.
2. In the details pane, click **SOFTLAYER**.
3. In the **Setup CloudBridge on SoftLayer wizard**, click **Next**, and then follow the instructions in the wizard.